A lot has happened in the past week or so.  It is hard to pick what might be the more interesting of the items.  I'll let you decide, but for me some key items include:

OHI Information Memo,  2002-001,  Fed. Extension - see attachment
OHI Policy memo, COHI PM-2002/0,  Workgroup Product  Approval
        Process - see attachment
CMS's What's New Site
California-Specific Privacy Seminars from CHA/CHIA
Tom Hanks - Info on Trans Rule,  Compliance Act and Sec &
        Priv  - See attachments
WEDI SNIP Updates
AFECHT Letter of January 25, 2002 - see attachment

As always:  Please be sure to note that in some cases the information presented may be the opinion of the original author.  We need to be sure to view it in the context of our own organizations and environment.  In some cases you may need legal opinions and/or decision documentation when interpreting the rules.

My thanks to all the folks who have shared information for this e-news.
Have a great day!!!
Ken


Interesting topics below:
OHI Information Memo,  2002-001,  Fed. Extension - see attachment
OHI Policy memo, COHI PM-2002/0,  Workgroup Product  Approval
        Process - see attachment
CMS's What's New Site
California-Specific Privacy Seminars from CHA/CHIA
Tom Hanks - Info on Trans Rule,  Compliance Act and Sec - Priv  - See
attachments
HIPAA Implementation Newsletter -- Issue #26 - January 25, 2002 - see
attachment
[hipaalive] RE: Privacy:  Sanction Policy
April 22-25, 2002 National Medicaid HIPAA and MMIS Conference
WEDI SNIP Updates
[hipaanotes] HIPAAnote - Vol. 2, No. 5 - 2/6/02
[hipaalive] Re: TCS: Certification
[hipaalive] RE: TCS:  EDI Question
[hipaalive] RE: TCS-DSM IV Psychiatric Coding
[hipaalive] RE: PRIVACY: Extensions for Privacy Regulations
AFECHT Letter of January 25, 2002 - see attachment


****************************** CMS's What's New Site
****************************

Health Care Financing Administration's Medicare Medicaid SCHIP What's New
Site Index
 http://www.hcfa.gov/medicare/edi/hipaadoc.htm

This has a lot of good information from CMS.   Their Home Page is:
  http://www.hcfa.gov/medicare/edi/edi.htm


******************** California-Specific Privacy Seminars from
CHA/CHIA ********************
>>> "Ginger Cox" <GCox@oshpd.state.ca.us> 01/29/02 03:06PM >>>
California Healthcare Association (CHA) is partnering with California Health
Information Association (formerly CA Medical Records Assoc.) on a seminar
regarding the HIPAA privacy rules from the hospital perspectives.

Initially there have been some concerns as to whether the hospitals can
release individually identifiable health information to the state.  We checked
this out - if it is required by state law, the hospitals are required to report it
to the state.  I doubt this will be raised again.  Starla Ledbetter, our HIPAA
Coordinator for OSHPD, (also a member of CHIA) will attend this seminar.

Invitation is open for anyone who is interested.  It looks like it will cover
hospital issues regarding pre-emption.

Ginger

===========================================
Ginger Cox, RHIT, CCS, Research Analyst II
Healthcare Information Division (HID)
Healthcare Quality and Analysis Division (HQAD)
Office of Statewide Health Planning and Development
818 K Street, Sacramento, CA  95814
916-327-3915 (FAX 916-327-1262) - HID (Monday-Thursday)
916-327-2249 (FAX 916-324-9242) - HQAD (Friday)
E-mail: gcox@oshpd.state.ca.us
Web: www.oshpd.state.ca.us

**********************************
************************************
************************
Helping Members Comply with Both Federal and California Privacy Laws

The California Healthcare Association (CHA) is pleased to partner with CHIA
to bring quality educational programs to those working in the complex area
of health care.  CHIA is a proud supporter of CHA's new HIPAA Privacy
Seminars.  These highly anticipated programs are California-specific and
will address the myriad of compliance issues with the HIPAA Privacy
Regulations effective April 14, 2003.

As a member of CHIA, you will be extended the discounted, CHA member rate of
$275 - a savings of $250 over the nonmember rate.

Health care providers face a huge task.  In just over a year they must comply with the new federal patient privacy laws under HIPAA - the Health Insurance Portability and Accountability Act.  Because California has long had patient privacy laws in place, this task is especially complex.  HIPAA requires that you follow whichever law (HIPAA or state law), or provision within the law, provides greater patient protection.

The good news is that CHA has done the work for our members in comparing HIPAA to California's Confidentiality of Medical Information Act (CMIA). The result is a detailed comparison of these laws - making this a must-attend seminar!

Seminar dates are:

* February 5, 2002:  Sacramento
* February 6, 2002:  San Ramon
* February 27, 2002:  Pasadena
* February 28, 2002:  Long Beach

For a brochure and/or registration form, visit the CHA website at:
<A HREF="http://www.calhealth.org/res_edu.htm">http://www.calhealth.org/res_edu.htm</A> and click on the HIPAA Privacy Seminar.
CEU's are available for lawyers, nurses, social workers, ACHE and AHIMA members.

If you have any questions, contact:

Mary-Anne Kelly
Director of Education
California Healthcare Association
Direct:    916-552-7500
Fax:        916-552-7506
E-mail:   <A HREF="mailto:mkelly@calhealth.org">mkelly@calhealth.org</A>


******* Tom Hanks - Info on Trans Rule,  Compliance Act and Sec - Priv
*****************
****************** SEE ATTACHMENT PDF's
************************************
Ken,

I have no problem with your sharing the document (re: "HIPAA Security and Privacy Rules: Working Together" dated Oct. 23, 2001) - I hope it helps.

I am also attaching a couple of other papers that address some of the issues surrounding the Transactions rule and the new Compliance Act.

(See attached file: Administrative Simplification Compliance Act - HR 3323 PwC Comments 010602.pdf)(See attached file: HIPAA Myths 010102.pdf)

I hope these help,

Thanks,

Tom Hanks
Director Client Services
Health Care Practice
PricewaterhouseCoopers, LLP
One North Wacker
Chicago, IL 60606
Email: Tom.Hanks@us.pwcglobal.com
www.pwcglobal.com/healthcare


******************** [hipaalive] RE: Privacy:  Sanction Policy
*********************
*** HIPAAlive! From Phoenix Health Systems/HIPAAdvisory.com ***
I have seen some good examples in the CPRI toolkit.  It is free and
is available on-line at cpri-host.org.  From the main page, just start
looking for the toolkit and you will eventually find some sample policies
and procedures.

Hope this helps,
Dan Kelsey
Data Projects Coordinator
Indiana State Medical Association


*********** April 22-25, 2002 National Medicaid HIPAA and MMIS
Conference ****************
>>> "Susan Fox" <susan@foxsys.com> 01/24/02 07:24AM >>>
Hope you can come. Please pass the word.

Susan Fox wrote:

> Registration for the 2002 National Medicaid HIPAA and MMIS Conference is
> now open.  This conference is hosted by the Centers for Medicare &
> Medicaid Services and the State of Maryland, Department of Health and
> Mental Hygiene.  Dates for the conference are April 22 - 25, 2002.

> Location is Mariott's Hunt Valley Inn, Hunt Valley, Maryland. The
> registration fee is $200 and the hotel's government rate is $110.
>
> For more information and to register on-line, visit
> http://www.hcfa.gov/medicaid/hipaa/adminsim/events.htm
>
> Reasons why you should attend this conference:
>
> * Learn about the most recent HIPAA requirements from the national
> experts who helped write them: including Privacy and Security, as well
> as the Transactions and Code Sets.
> * Participate in interactive, hands-on workshops with state, federal,
> and private representatives working collaboratively to strategize on:
>      -Medicaid cost containment
>      -MMIS contracting
>      -How to get the marketplace to convert to electronic exchange
> of data
>      -Using commercial software to improve operations in the  MMIS
>      -Receive the latest updates from the National Medicaid EDI
> HIPAA (NMEH) Chairs, discuss and field questions to help implement
> your programs.
>      -Hear practical and proven approaches to addressing      common
> problems and solving them quickly and efficiently.
>      -Discover what industry leaders outside of Medicaid are doing
> that has practical implications for your world.
>       -Leverage HIPAA possibilities to position your organization after HIPAA.
>      -Join with your colleagues in networking opportunities where
> talk is bound to be lively and informative.
>
> Hope to see you there!

Susan J. Fox
Fox Systems Inc.
4110 N. Scottsdale Rd.
Suite 355
Scottsdale, AZ 85251
susan.fox@foxsys.com


*********************************************** WEDI SNIP Updates
*******************************
WEDI SNIP Announces a new webcast: Testing Compliance, Certification, and
Business to Business Testing.  This webcast will be held from 2:00 - 3:30
EST, on February 28.  For more information visit <A
HREF="http://snip.wedi.org/public/articles/details.cfm?id=372">
http://snip.wedi.org/public/articles/details.cfm?id=372</A>.

The latest SNIP Synopsis is now available online.  To view a .pdf version, visit <A HREF="http://snip.wedi.org/public/articles/12902.pdf">http://snip.wedi.org/public/articles/12902.pdf</A>.  To download the Word document version, visit <A HREF="http://snip.wedi.org/public/articles/SNIPSynopsis012902.doc">http://snip.wedi.org/public/articles/SNIPSynopsis012902.doc</A>.

Don't forget to register for the WEDI SNIP Special Payers Forum and the March
Forum.  Hotel reservations must be made by February 10.  For more information, visit <A HREF="http://snip.wedi.org/public/articles/index.cfm?Cat=38">http://snip.wedi.org/public/articles/index.cfm?Cat=38</A>.


* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
* * * * * * * * *


* * * * * * * * * * * * * * * * * * *  [hipaanotes] HIPAAnote - Vol. 2, No. 5 - 2/6/02
* * * * * * * * * * * * * * * * * * * * * * * * *
>>> <info@phoenixhealth.com> 02/06/02 07:35AM >>>
==================================================================
H I P A A N O T E -- Volume 2, Number 5 -- February 6, 2002

>> From Phoenix Health Systems...HIPAA Knowledge...HIPAA Solutions <<
        > Healthcare IT Consulting & Outsourcing <
==================================================================
This week's HIPAAnote...

*** HIPAA Security: Not Just About Villains ***

Ask people about the purpose of a security program, and you may conjure up thoughts of Agent 007. James Bond used high tech tools and his wits to defeat the nastiest of villains. In the real world, a good security program should address all types of threats - from the most malicious to the accidental. Security experts commonly categorize these threats as one of the following:

• Direct Threats

• Indirect Threats

• Acts of God

• Human Nature

Direct Threats occur when an individual attempts to gain unauthorized access to, or get possession of your assets. The direct threat often receives the most attention because it is easiest to identify. Within health care, direct threats may take the form of hackers attempting to break into your computers, the theft of a personal computer, or entering a secure area. Keep in mind that your assets don't have to be tangible to be real; the value of your reputation and your information may be higher than the value of your equipment.

Indirect Threats are random situations where your organization is not specifically an intended target. "Catching" a computer virus is likely the result of an indirect threat. The theft of an unattended PDA may also be the result of an indirect threat if the thief was not looking for that PDA when they stumbled across it.

Protecting your organization against Acts of God requires an acknowledgement of natural events and their potential impact. The use of emergency generators can help reduce the impact of a potential power outage. Backup tapes of sensitive computer data reduce the risk of loss in the event of a disk drive failure. Disaster recovery plans are developed specifically against this type of threat.

Finally, Human Nature creates many organizational security risks. Lack of training, poorly documented or executed procedures, simple carelessness, or mistakes in judgment cause the great majority of security incidents within organizations.

The HIPAA Security NPRM is designed to address all four threat categories. Given the recent rumblings that the final Rule will be published soon, you should start looking NOW at how security threats could impact your organization.

That's today's HIPAAnote...now, pass it along!

==============================
HIPAAnotes are published weekly as a learning tool to help you and your associates stay tuned-in to HIPAA and its implications. Forward it to anyone with a "need to know" through your own internal mailing list, intranet or newsletter -- whatever works for you....

Our HIPAAcratic oath: We'll use your ideas for HIPAAnotes -- send them!
E-mail D'Arcy Gue, Editor: info@phoenixhealth.com
==============================

==================================
To view the list's archives, change your settings, or unsubscribe, go to:

http://lyris.dundee.net/cgi-bin/lyris.pl?enter=hipaanotes


\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* [hipaalive] Re: TCS: Certification
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*
\*\*\* HIPAAlive! From Phoenix Health Systems/HIPAAdvisory.com \*\*\*
WEDi-SNIP is offering a Web cast on this topic in February.
http://snip.wedi.org/public/articles/details.cfm?id=372

Marcallee Jackson
Long Beach, CA
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* [hipaalive] RE: TCS:  EDI Question
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*
\*\*\* HIPAAlive! From Phoenix Health Systems/HIPAAdvisory.com \*\*\*

The HIPAA transactions rules apply differently depending on the type of
entity.

A health plan is required to be able to conduct all of the HIPAA
transactions electronically, in HIPAA standard format, by the compliance
data.  The only exception is that a health plan is not required to implement
the capability to conduct an electronic transaction if they don't conduct
the transaction at all.  For instance, if a health plan does not require
pre-authorizations or referrals as preconditions to paying certain types of
claims, they do not have to implement the HIPAA referral transaction.  Also,
the regulations say that a health plan must conduct the HIPAA standard
transaction "if an entity requests" it to do so.  So a group health plan
that is operated by an employer only for its own employees, may know with
certainty that the only entity with whom it conducts electronic enrollment
transactions, the employer that operates the health plan, will not request
it to conduct enrollment in HIPAA-standard format.  In this case, the health
plan would not need to implement that standard.

A covered provider is required to conduct electronic transactions in
HIPAA-standard format.  But it is not required to conduct any of these
transactions electronically.  So the provider has the option of doing some
transactions electronically (in standard format) and some manually.  This
also includes the same type of transaction in different situations.  A
provider may conduct claims transactions electronically with one payer, and
manually with another.  Or it may conduct certain types of claims
electronically, and others manually, with the same payor.  However, if the
provider conducts the transaction electronically, it must be in
HIPAA-standard format.

An employer (other than a covered provider, health plan, or clearinghouse)
is not a covered entity.  So employers may continue to conduct transactions
electronically in non-standard format with covered entities.  An employer

has the option of requesting a health plan to conduct enrollment transactions in the 834 standard, or to conduct enrollment using a flat file or other non-standard electronic format, or manually, or some combination of these. The health plan is required to honor the request to do the 834 transactions. It is a business decision whether to continue to support non-standard formats for its transactions with employers.

In the context of your e-mail, this raises an interesting question regarding covered entities who are also employers. If Amalgamated Widgets wants to use a non-standard format to do electronic enrollment, that is between it and the health plan. But if Amalgamated Hospital wants to use a non-standard format for electronic enrollment in its health plan, it is prevented from doing so, since it is a covered provider. Covered providers may not conduct transactions in non-standard format when HIPAA has established a standard.

The hybrid entity rule applies to entities whose primary purpose is not health care, but which have a health component. For instance, Amalgamated Widget has a group health plan. It is a hybrid entity, in which the group health plan is subject to HIPAA. But the rest of the company is not subject to HIPAA. However, I do not see how a covered entity, such as a hospital, could reverse that argument, and claim that certain functions were not HIPAA covered functions. That is, I don't believe that a hospital can claim that, when it is acting as an employer, it is not acting as a covered entity, and doesn't have to use HIPAA-standard transactions in the context of its employer role. In the preamble discussion of the hybrid entity concept, it states: "Is most of what the covered entity does related to its health care functions? If so, then the whole entity should be covered." [65 FR 82502 (12/28/00)]

Bill


William A. MacBain
Principal
MacBain & MacBain, LLC
1108 Hector St.
Ithaca, NY 14850
607-256-1522


-----Original Message-----
From: Karl Pfaehler [mailto:kpfaehler@SCHA.org]
Sent: Monday, January 28, 2002 8:50 AM
To: HIPAAlive Discussion List
Subject: [hipaalive] TCS: EDI Question

*** HIPAAlive! From Phoenix Health Systems/HIPAAdvisory.com ***

Are the HIPAA regulations in regards to EDI an all-or-non rule? For example, if a CE has multiple care facilities, i.e. extended care, acute care facility, community medical centers, outpatient surgery centers, and physician practices, do they have to convert from a manual process in one area, such as their human resources division, and go with electronic filing in the 834 format, as opposed to maintaining the manual process via sending a flat file to the insurance carrier? I am trying not to split hairs, but this is not crystal clear to me. The same CE files the biggest portion of its claims remittance information via electronic process. With this in mind, can they continue with a  manual process in one area and electronic in another? How are insurance carriers handling this in regards to businesses that are non-health care related when it comes to benefit enrollments and benefit modifications?


Karl Pfaehler, CPHRM, FASHRM
Risk Management Coordinator for Clinical Services
South Carolina Hospital Association

******************** [hipaalive] RE: TCS-DSM IV Psychiatric Coding
*****************************
*** HIPAAlive! From Phoenix Health Systems/HIPAAdvisory.com ***
TCS-DSM IV Psychiatric CodingDSM-IV is a subset of the ICD-9-CM, which is an approved code set.  You can get more information at:

http://www.psych.org/clin_res/q_a.cfm#Medicare,%20Medicaid

Jeffrey Young
BEST Consulting


******************** [hipaalive]  PRIVACY: Extensions for Privacy
Regulations ************
*** HIPAAlive! From Phoenix Health Systems/HIPAAdvisory.com ***

Extensions for Privacy Regulations:    There is no provision for extensions under
the privacy regulations.  Covered entities (except for small health plans) must comply by 4/14/03.  Small health plans get an extra year.

I would also be skeptical of an information system that is going to plug privacy gaps.  With a few exceptions, such as electronic tracking of reportable disclosures, compliance with the privacy regulations is a matter of policies, procedures, training and forms development -- not information

system modifications.

Bill

William A. MacBain
Principal
MacBain & MacBain, LLC

********************* [hipaanotes] HIPAAnote - Vol. 2, No. 4 - 1/23/02
****************************
=================================================
==================
H I P A A N O T E -- Volume 2, Number 4 -- January 23, 2002

>> From Phoenix Health Systems...HIPAA Knowledge...HIPAA Solutions <<
       > Healthcare IT Consulting & Outsourcing <
=================================================
==================
** "Between a Rock and a Hard Place:
Assessing the Impacts of the TCS Compliance Extension" AudioConference **

Join us for this intensive 60-minute audio discussion + presentation
slides by Phoenix Health Systems' Principal Clyde Hewitt
TOMORROW, January 24 at 2:00 PM EST

SIGN UP NOW! Go to: http://www.hipaadvisory.com/ezcart/index.cfm?0123n
=================================================
==================

This week's HIPAAnote...

*** HIPAA Terms: Implementing Effective HIPAA Policies - Part II ***

In the last HIPAAnote we discussed why privacy and security policies are
critical to HIPAA compliance, and the difference between a "policy" and a
"procedure." This HIPAAnote looks at the characteristics of effective
policies, and steps needed to implement them.

Effective policies should:

· be sanctioned, published, promulgated, and given visible support by top
management.
· cover all the pertinent requirements of management concerning the
subject matter.
· not include operational details that may vary from time to time
· meet the test of uniformity (apply consistently across all affected
areas).

· meet the test of observance (workforce knows of them and follows their prescriptions).
· meet the test of longevity (should seldom have to be changed), but are revisable as requirements change.

Because policies will affect most, if not all, the organization's workforce, stakeholder representatives should be part of the process of policy development and endorsement.  One approach is to utilize a committee (Security and Confidentiality), making sure it includes your Privacy Officer and Security Officer.

To create policies:

· Establish a formal project to develop policies.
· Obtain support and involvement of management.
· Read and understand the original HIPAA regulatory text on the issue at hand.
· Research the issue and how others have addressed it. Don't assume you must re-invent the wheel. Sample approaches abound at the Web sites of many industry associations (AHIMA, AHA, AAMC), government agencies (NIST,
NIH, and state HIPAA sites), other HIPAA-focused organizations (WEDI-SNIP and regional HIPAA initiatives) and private sector sites (e.g. security and law firms). But, a word of caution. Every covered entity is unique, and policies must reflect its particular needs, environment, and culture. Tailor your policies to your organization.
· Draft the policies for committee review and approval. Make them short (one to two pages), and written in plain language that anyone can read and understand.
· Follow your organization's review and approval process (including Legal).

Set a timetable for announcing approved policies PRIOR to relevant compliance dates. Announcements should come from senior management, and
should reference the procedures to come that will facilitate compliance.

If policies are to become an integral part of the organizational fabric, they must be included in employee orientation and staff training programs. This is not just a "good idea;" the framers of HIPAA were so aware that behavioral change takes time and reinforcement that training of every workforce member on HIPAA policies is a requirement. And, should violations occur, it is equally necessary that enforcement and sanctions follow.

To learn more about implementing privacy and security policies and procedures, go to:
http://www.hipaadvisory.com/action/index.htm?0123n

That's today's HIPAAnote...now, pass it along!